IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Moon et al.	Attorney Docket No.: CISCP361/8157
Application No.: 10/758,757	Examiner: Ellen C. Tran
Filed: January 15, 2004	Group: 2134
Title: ESTABLISHING A VIRTUAL PRIVATE NETWORK FOR A ROAD WARRIOR	Confirmation No. 6416

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on April 18, 2007.

Signed: /Kristina Gomez/
Secretary

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reasons stated below.

The Examiner rejected claims 1, 4, 6, 8-12, 15, 17 and 19-20 under 35 U.S.C. 103(a) as being unpatentable over Ahonen (6,976,177).

The Examiner rejected claims 2, 3, 5, 13, 14 and 16 under 35 U.S.C. 103(a) as being unpatentable over Ahonen (6,976,177) in view of Subramaniam et al. (6,640,302).

The Examiner rejected claims 7 and 18 under 35 U.S.C. 103(a) as being unpatentable over Ahonen (6,976,177) in view of Jari et al. (6,907,532).

An Office Action was issued on July 24, 2006 and a Final Office Action was issued on December 8, 2006 outlining substantially the same rejections as each other. In response to the

earlier Office Action, Applicant argued that the prior art does not teach or suggest various elements of the claims because Ahonen fails to teach or suggest the use of a shared secret.

The Final Office Action responded to the Applicant's arguments by stating "[t]he Examiner disagrees the shared secret [in Ahonen] is the Security Association (SA), see col. 1, lines 45-67" and "[t]he Examiner disagrees with argument, and notes again the shared secrets are the SAs, which due (sic) incorporate certificates."

Applicant responded to the Final Office Action by pointing out that there appeared to be some confusion regarding the term "shared secret," as that term cannot possibly refer to a security association. In an advisory action mailed on February 22, 2007, the PTO responded by arguing that a shared encryption method is a shared secret.

Applicant respectfully points out that the PTO has now apparently identified three separate elements in Ahonen as allegedly teaching a "shared secret". Each time Applicant has pointed out that the alleged element in Ahonen did not equate with a shared secret, the PTO has responded by selecting a different element in Ahonen to equate with a shared secret. As a threshold matter, Applicant respectfully believes that it is necessary for the PTO to arrive at a definite reason for rejection so that Applicant can properly respond. As such, Applicant respectfully requests that the PTO specifically identify which element in Ahonen is allegedly a shared secret. Is it the security association itself, a certificate, or a shared encryption method (or some other element)? Without this information, Applicant does not believe that prosecution can continue further.

Nevertheless, Applicant maintains that none of the elements in Ahonen equate with a shared secret.

"Shared secret" is a term known in the art and refers to a type of authentication, similar to a password. Evidence of this can be provided upon the Examiner's request. There are of course numerous different types of authentications, including passwords, shared secrets, and certificates. Each of these types of authentication is different from each other and perhaps more importantly, each of them is different than a security association. A security association is a mapping of certain agreed-upon parameters with two or more entities that will share the parameters. It is essentially an agreement between two or more network entities to use certain settings, protocols, etc. for communication. An authentication is something that is used to authenticate the user or device that will be used in a security association, but equating a security

association with a shared secret is no more correct than equating a security association with a password. They are simply different types of entities.

In Ahonen, certificates are utilized to create multiple security associations. The certificates are the authentications and the security associations are the end goals of the authentication process. A shared secret can only refer to a type of authentication and not to an end goal of an authentication process. As such, Applicant respectfully submits that a security association itself is not a shared secret.

Agreeing on a shared encryption method, which the PTO argues in the Advisory Action is equivalent to a shared secret, is also not a shared secret. First, an agreed-upon encryption method is only utilized once a security association has been established. A shared secret, on the other hand, is a method of authentication that occurs before a security association is established. Nevertheless, the encryption method is not secret. Only the actual key/password/certificate used in the encryption method is secret, but the method being used is not secret. For example, in password-based authentication, anyone who attempts to establish a security association is prompted for a password. Thus, everyone who tries to establish a security association is able to see that the encryption method is password-based. The same occurs for key-based and certificate-based authentication/encryption.

Specifically, claim 1 contains the following elements that cannot be taught by a reference lacking a shared secret: "establishing a correspondence between the IP address and a first shared secret authorized for the user," "receiving a second request from the user to form a virtual private network tunnel, the request incorporating a second shared secret," "determining whether the first shared secret matches the second shared secret," and "forming the virtual private network tunnel when the first shared secret matches the second shared secret."

In short, a shared secret is an authentication method. Attempting to equate a shared secret with anything other than an authentication method is clearly incorrect. Furthermore, even the elements of the prior art that do teach authentication methods are teaching certificates, which are not the same as shared secrets.

Nevertheless, the rejections to date are extremely confusing and are inconsistent as to the basis for the rejection. Each of the office actions/advisory actions state a different basis for the rejection, including different elements from Ahonen. The advisory action even refers to the

"typical SA", describing elements not in any of the cited prior art, apparently taking official notice of some fact that is unknown to the applicant.

As such, Applicant respectfully maintains that claim 1 is in condition for allowance.

As to independent claims 12, 19, and 20, these claims contain elements similar to that as described above with respect to claim 1, and as such Applicant respectfully submits that these claims are also in condition for allowance.

Dependent claims 2-11 and 13-18 are also patentably distinct from the cited references for at least the same reasons as those recited above for the independent claim, upon which they ultimately depend. These dependent claims recite additional limitations that further distinguish these dependent claims from the cited references. For at least these reasons, claims 2-11 and 13-18 are not anticipated or made obvious by the prior art outlined in the Office Action.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. In lieu of a Notice of Allowance, Applicant notes that this response puts the application in a better condition for appeal and respectfully requests that it be considered and entered. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

I am the attorney or agent acting under 37 CFR 1.34

Respectfully submitted,
BEYER WEAVER LLP

/Marc S. Hanish/
Marc S. Hanish
Reg. No. 42,626

P.O. Box 70250
Oakland, CA 94612-0250
408-255-8001